Claims

1. (Currently amended) Method for encrypting data in a communication network comprising a device of a first type comprising steps for:~~containing~~:

- a first symmetric key that is used for encrypting the data to be sent to a device of a second type connected to the network, wherein said second type of device is a different device type from said device of a first type; and

- and an encrypted first symmetric key ~~which is~~ generated from the encryption of said first symmetric key with a second symmetric network key known ~~only~~ by ~~at least one device of a~~ the second type connected to said network;

the method ~~comprising the steps~~ ~~for~~ performed by the device of ~~a~~ the first type of comprising the additional steps:

(a) generating a random number;

(b) computing a new symmetric key as a function of the first symmetric key and said random number;

(c) encrypting the data to be transmitted with the new symmetric key; and

(d) transmitting to a device of a second type, via said network:

- the data encrypted with the new symmetric key;

- the random number; and

- said encrypted first symmetric key.

2. (Previously amended) Method according to claim 1, wherein the function used to compute the new symmetric key is a one-way derivation function.

3. (Previously amended) Method according to claim 2, wherein the function is a hash function.

4. (Previously amended) Method according to claim 1, also comprising the steps for the device of a second type that receives data transmitted at step (d) of :

(e) decrypting, with the second symmetric network key the encrypted first symmetric key as to produce the first symmetric key;

(f) determining, based on the first symmetric key obtained at step (e) and on said random number, the new symmetric key; and

(g) decrypting the data received with the new symmetric key.